REMARKS

The Office Action of September 15, 2008 (Paper No. 20080911) has been carefully considered.

The claims are not amended. Thus, claims 5-8 are pending in the application.

Claims 5-8 are rejected under 35 U.S.C. 102 for alleged anticipation by Sasmazel, European Patent Application No. 1328101A2. For the reasons stated below, it is submitted that the invention as claimed is distinguishable from the cited reference so as to preclude rejection under 35 U.S.C. 102 or 103.

The cited reference, Sasmazel '101, presents a set of equipment which realizes coded information transfer with a combination of centralized communication networks similar to the traditional telephone system and the TAN number system known in the financial community. The disadvantage of the method and apparatus of Sasmazel '101 is that is uses a single-key algorithm for the coding of communications, and it stores all of the keys in a single place in a main element of the system, the call complex 102 of Figure 1 of the reference. Furthermore, all of the communication occurring in the system travels through the call complex 102. As a result, the system of Sasmazel '101 is vulnerable because, if the call complex 102 is controlled by an unauthorized person, or if the keys stored in the call complex 102 are illegally possessed, all of the communications taking place in the network

can be decoded by unauthorized persons. Thus, the call complex 102 of Sasmazel '101can become a primary target for access attacks.

A further disadvantage of the method and apparatus of Sasmazel '101 is that it is the call complex 102 itself that initiates communication in order to establish calls with called end terminals. This makes the call complex 102 vulnerable to well-known hacker techniques. Another serious security flaw in the method and apparatus of Sasmazel '101 is that all of the section keys required for the interpretation of communications are transmitted over the communication channel of the call complex 102 through a set network point, even though coded. The section keys also pass through the network during the call establishment process. This characteristic also creates an opportunity for potential attack. In addition, the method and apparatus of Sasmazel '101 uses the same section key for both directions of communication (see SKLST[n] of Figure 3 of the reference) so that acquisition of one key makes it possible to eavesdrop on the entire communication.

A further disadvantage of the method and apparatus of Sasmazel '101 is that, since all communication is carried out through the call complex 102, the data transfer capacity of the call complex is continually burdened in proportion to the number of communications taking place at any specific point in time. As a result of the above security deficiencies, the method and apparatus of Sasmazel '101 are not suitable for creating a secure, general-purpose Internet Protocol (IP)-based network with system-level protection. In contrast, the disadvantages and deficiencies of the method and apparatus of Sasmazel '101, including its security flaws, do not occur in the present invention.

Specifically, in the present invention, only asymmetric keys are used for securing the system. The keys required for the decoding and interpretation of communications never pass through the communication network while the system is operating, and the decoding keys never leave the end terminals or the central traffic coordination unit. Moreover, these keys cannot be found together at any single point in the system so that, in accordance with the invention, the set of devices has no point in it which can be broken into. As a result, it is not possible for all communications in the system to be illegally decoded. Furthermore, even if the central traffic coordination unit or data stored therein were to become illegally possessed, it would still be impossible to decode communications taking place in the system.

Furthermore, in the present invention, the central traffic coordination unit is essential and unavoidable for the construction of the communication channel between the end terminals, but the constructed communication channel does not pass through the central traffic coordination unit so that communication between the end terminals takes place directly between the end terminals. Accordingly, simultaneous instances of communication only use the capacity of the central traffic coordination unit when constructing the communication channel, but do not use it when the communication is taking place.

In addition, in accordance with the present invention, there is no single network point through which all communication channels pass. A further significant difference between the claimed invention and the prior art is that, in the invention, the central traffic coordination unit never initiates communication so that the central traffic coordination unit is protected against attacks that use communication initiation.

Due to these important and basic differences between the invention and the prior art, it can be concluded that the locations and "movement" of the code keys employed in the invention could not be set up in the apparatus and method disclosed in Sasmazel '101, as well as in other prior apparatuses and methods. This is due to the fact that the structure of the invention, the location of the code keys, and the movement thereof differs from those of known systems, resulting in achievement of an inventive step not found in prior systems.

It should be noted that the above arguments were presented to the International Preliminary Examining Authority (IPEA) in order to overcome a rejection of the corresponding international application based on the same reference (Sasmazel '101), and that the claims of the corresponding international application recite the same subject matter as, and are virtually identical to, the claims pending in the present application. Moreover, it should also be noted that the international claims were accepted by the European Patent Office (EPO) and that, as a result, a European patent was granted and was validated in more than twenty (20) European countries. Therefore, for the same reasons that the claims of the international application were allowed and were validated throughout Europe, the present U.S. claims should also be allowed.

However, there are additional reasons for distinguishing the invention claimed herein from the cited prior art. Specifically, on page 3 of the Office Action, the Examiner alleges that each transmitting terminal device (end unit 110 of Figure 1) includes a receiver partial unit and a storage partial unit, the Examiner citing column 5, lines 35-45 and column 8, lines 23-32 of Sasmazel '101. However, such is not the case because column 5, lines 35-45 of

Sasmazel '101 only discloses a memory 202 contained in the call complex 102 which, according to the Examiner's analysis, corresponds to the claimed central traffic coordination unit, while column 8, lines 23-32 does not mention any receiver partial unit or storage partial unit at all. Thus, Sasmazel '101 does not disclose or suggest a receiver partial unit and/or a storage partial unit in a transmitting terminal device, as recited in independent claim 5.

In addition, at page 3, lines 6-8 of the Office Action, the Examiner alleges that Sasmazel '101discloses that a storage partial unit in a transmitting terminal device includes a D-register containing a device identical signal, but (as mentioned above) Sasmazel '101 does not disclose a storage partial unit in a transmitting terminal device, and in fact it does not disclose a D-register in any storage partial unit.

Furthermore, in making the above assertion, the Examiner cites column 11, lines 1-10 for the alleged disclosure of a request containing a terminal ID and an IP address code but those items are not found at column 11, lines 1-10 of Sasmazel '101.

Moreover, at page 3, lines 11-19 of the Office Action, the Examiner alleges that Sasmazel '101 discloses a C-register storing a coding key and connected to a sender partial unit (citing Figure 1 of the reference). However, a review of Sasmazel '101 reveals that the memory for storing a coding key, as contained in call complex 102, is not connected to end unit 110, or to any sender partial unit contained therein.

In addition, in the paragraph bridging pages 3 and 4 of the Office Action, the Examiner alleges that Sasmazel '101 discloses a storage partial unit of each transmitting terminal device which includes at least one temporary storage register for the temporary

storage of coding keys of other transmitting terminal devices, citing column 11, lines 20-30 of the reference. However, the end unit identification code referred to at column 11, lines 20-21 of Sasmazel '101 is not a key for encoding/decoding transmissions, but rather it is the identification code for end unit 2 as stored in end unit 2 itself. Moreover, it does not constitute a coding key of other end units or transmitting terminal devices as alleged by the Examiner.

On page 4 of the Office Action, the Examiner refers to the call complex 102 as having an MD-register for storing a master code key, and also refers to the end units as having C-registers. However, none of the cited portions of Sasmazel '101 discloses or suggests C-registers or D-registers.

In addition, in the paragraph bridging pages 4 and 5 of the Office Action, the Examiner alleges that, in the storage partial unit of a first transmitting terminal device, there is only information free from the coding key of the first transmitting terminal device, the Examiner citing column 8, lines 15-25 of Sasmazel '101. However, the cited portion of Sasmazel '101 merely discusses encryption, transmission of an authorization request, and identification of the request, but does not at all disclose or suggest that there is, in a storage partial unit of a first transmitting terminal device, only information free from the coding key of a first transmitting terminal device.

Furthermore, referring to page 5, lines 1-3 of the Office Action, there is no disclosure or suggestion of a temporary storage register of a first transmitting terminal device, and the

end-unit-to-end-unit session key referred to at cited column 8, lines 35-45 of Sasmazel '101 is not a coding key of a first transmitting terminal device, as alleged in the Office Action.

At page 5, lines 4-9 of Office Action, the Examiner alleges that Sasmazel '101 discloses that only the coding key of the first transmitting terminal device (end unit) participating in an information exchange is temporarily stored in a temporary storage register of a second transmitting terminal device, the Examiner again citing column 11, lines 35-45 of the reference. However, such a temporary storage register of a transmitting terminal device is not disclosed in the cited portion of Sasmazel '101, or in Sasmazel '101 in its entirety. Furthermore, the cited portion of Sasmazel '101 does not refer to a coding key of a first transmitting terminal device, but rather refers to an end unit to end unit session key EUEUSK.

For the reasons stated above, it is respectfully submitted that, contrary to the assertions in the Office Action, Sasmazel '101 does not disclose or suggest the invention as recited in independent claim 5. Therefore, a rejection under 35 U.S.C. 102 or 103 is inappropriate.

In addition, the dependent claims of the present application further distinguish the invention from the cited prior art. Specifically, referring to dependent claim 6, at page 5, lines 17-19 of the Office Action, it is alleged that Sasmazel '101 discloses temporary storage registers of transmitting terminal devices connected to a sender partial unit, citing Figures 1-3 of the reference. However, as indicated above, Sasmazel '101 does not disclose sender partial units of terminal devices, and therefore there is no disclosure or suggestion of

temporary storage registers of transmitting terminal devices connected to a sender partial unit.

In the view of the above, it is submitted that the claims of the present application are in condition for allowance, and early issuance of this application is solicited.

No fee is incurred by this Response.

Respectfully submitted,
Miklós JOBBÁGY et al

By: _____
Joseph G. Seeber
Reg. No. 27,719

Post Office Box 750
Great Falls, VA 22066
Telephone: (703)430-1702
Facsimile: (703)450-7914